No. 15-2560

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION, *et al.*,

Plaintiffs–Appellants,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants–Appellees.

On Appeal from the United States District Court for the District of Maryland Baltimore Division

BRIEF FOR PLAINTIFFS–APPELLANTS

Patrick Toomey
Jameel Jaffer
Alexander Abdo
Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
ptoomey@aclu.org

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
jeon@aclu-md.org

Counsel for Plaintiffs–Appellants
(additional counsel on reverse)

Charles S. Sims
David A. Munkittrick
Proskauer Rose LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
csims@proskauer.com

Counsel for Plaintiffs–Appellants

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 15-2560 Caption: Wikimedia Foundation, et al. v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Amnesty International USA
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/Patrick Toomey Date: December 22, 2015

Counsel for: Amnesty International USA

CERTIFICATE OF SERVICE

****

I certify that on December 22, 2015 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave NW, Rm 6102
Washington, D.C. 20001

s/Patrick Toomey
(signature)

December 22, 2015
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 15-2560 Caption: Wikimedia Foundation, et al. v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Global Fund for Women
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/Patrick Toomey Date: December 22, 2015

Counsel for: Global Fund for Women

CERTIFICATE OF SERVICE

****

I certify that on December 22, 2015 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave NW, Rm 6102
Washington, D.C. 20001

s/Patrick Toomey
(signature)

December 22, 2015
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 15-2560 Caption: Wikimedia Foundation, et al. v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Human Rights Watch, Inc.
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/Patrick Toomey Date: December 22, 2015

Counsel for: Human Rights Watch, Inc.

CERTIFICATE OF SERVICE

****

I certify that on December 22, 2015 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave NW, Rm 6102
Washington, D.C. 20001

s/Patrick Toomey
(signature)

December 22, 2015
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 15-2560 Caption: Wikimedia Foundation, et al. v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

The Nation Company, LLC
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/Patrick Toomey Date: December 22, 2015

Counsel for: The Nation Company, LLC

CERTIFICATE OF SERVICE

****

I certify that on December 22, 2015 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave NW, Rm 6102
Washington, D.C. 20001

s/Patrick Toomey
(signature)

December 22, 2015
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 15-2560 Caption: Wikimedia Foundation, et al. v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

National Association of Criminal Defense Lawyers (NACDL)
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☑ YES ☐ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

None

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/Patrick Toomey Date: December 22, 2015

Counsel for: NACDL

CERTIFICATE OF SERVICE

****

I certify that on December 22, 2015 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave NW, Rm 6102
Washington, D.C. 20001

s/Patrick Toomey
(signature)

December 22, 2015
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 15-2560 Caption: Wikimedia Foundation, et al. v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

PEN American Center
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/Patrick Toomey Date: December 22, 2015

Counsel for: PEN American Center

CERTIFICATE OF SERVICE

****

I certify that on December 22, 2015 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave NW, Rm 6102
Washington, D.C. 20001

s/Patrick Toomey
(signature)

December 22, 2015
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 15-2560 Caption: Wikimedia Foundation, et al. v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

The Rutherford Institute
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/Patrick Toomey Date: December 22, 2015

Counsel for: The Rutherford Institute

CERTIFICATE OF SERVICE

****

I certify that on December 22, 2015 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave NW, Rm 6102
Washington, D.C. 20001

s/Patrick Toomey
(signature)

December 22, 2015
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 15-2560 Caption: Wikimedia Foundation, et al. v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Washington Office on Latin America, Inc. (WOLA)
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/Patrick Toomey Date: December 22, 2015

Counsel for: WOLA

CERTIFICATE OF SERVICE

****

I certify that on December 22, 2015 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave NW, Rm 6102
Washington, D.C. 20001

s/Patrick Toomey
(signature)

December 22, 2015
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 15-2560 Caption: Wikimedia Foundation, et al. v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Wikimedia Foundation
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/Patrick Toomey Date: December 22, 2015

Counsel for: Wikimedia Foundation

CERTIFICATE OF SERVICE

****

I certify that on December 22, 2015 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Ave NW, Rm 6102
Washington, D.C. 20001

s/Patrick Toomey
(signature)

December 22, 2015
(date)

TABLE OF CONTENTS

STATEMENT OF JURISDICTION...1

STATEMENT OF THE ISSUE 1

STATEMENT OF THE CASE 1

I. Introduction..1

II. Statutory Background 4

A. The Foreign Intelligence Surveillance Act of 1978 4

B. The Warrantless Wiretapping Program..6

C. The FISA Amendments Act of 2008 6

III. Statement of the Facts...10

A. The Government's Implementation of the FISA Amendments Act 10

B. Upstream Surveillance 11

C. Plaintiffs' Communications..15

IV. Procedural History 18

SUMMARY OF THE ARGUMENT 19

STANDARD OF REVIEW 22

ARGUMENT 22

I. The district court erred in holding that Plaintiffs had not plausibly alleged the copying and review of their communications 22

A. Legal standards..22

B. Wikimedia has plausibly alleged that the government is copying and reviewing at least some of its trillion or more international communications 24

1. Wikimedia's communications traverse every major internet circuit entering or leaving the United States 25

2. As a technological matter, the NSA must copy and review all international text-based communications transiting each of the circuits it monitors 27

3. For additional reasons, it is clear that the NSA is copying and reviewing at least some of Wikimedia's trillion-plus international communications 33

4. Wikimedia's standing allegations are plausible 37

C. Plaintiffs have also plausibly alleged that the NSA is copying and reviewing "substantially all" international text-based communications, including their own 40

1. The unpredictable routing of internet traffic requires comprehensive surveillance of international communications for Upstream surveillance to operate as the government has described 41

2. The structure of the internet backbone facilitates comprehensive surveillance of Americans' international communications 45

3. Plaintiffs' allegations that the NSA is intercepting substantially all international text-based communications are plausible 46

II. The district court erred in holding that *Amnesty International USA* forecloses Plaintiffs' standing 49

III. Plaintiffs have plausibly alleged standing for additional reasons 55

A. Plaintiffs have plausibly alleged that they have been compelled to take burdensome and costly measures in response to Upstream surveillance 55

B. Plaintiffs have plausibly alleged that Upstream surveillance impairs their protected expressive activities 58

C. Plaintiffs have plausibly alleged that the NSA is not only copying and reviewing their communications, but retaining them as well..59

D. Wikimedia has plausibly alleged third-party standing to assert the rights of its community members 61

CONCLUSION 61

REQUEST FOR ORAL ARGUMENT 63

CERTIFICATE OF COMPLIANCE 64

TABLE OF AUTHORITIES

Cases

[Redacted], No. [Redacted],
2011 WL 10945618 (FISC Oct. 3, 2011) .... passim

ACLU v. NSA,
438 F. Supp. 2d 754 (E.D. Mich. 2006) 6

Adams v. Bain,
697 F.2d 1213 (4th Cir. 1982) 23

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 23, 24, 38

Berger v. New York,
388 U.S. 41 (1967) 60

Clapper v. Amnesty International USA,
133 S. Ct. 1138 (2013) .... passim

Columbia Gas Transmission Corp. v. Drain,
237 F.3d 366 (4th Cir. 2001) 22

Cooksey v. Futrell,
721 F.3d 226 (4th Cir. 2013) .... passim

Friends of the Earth v. Laidlaw Envtl. Servs. (TOC), Inc.,
528 U.S. 167 (2000) 55

Goldfarb v. Mayor & City Council of Balt.,
791 F.3d 500 (4th Cir. 2015) 23

Houck v. Substitute Tr. Servs., Inc.,
791 F.3d 473 (4th Cir. 2015) 24, 48

In re [*Redacted*],
No. [Redacted] (FISC Apr. 3, 2007) 6

In re DNI/AG Certification [*Redacted*],
No. 702(i)-08-01 (FISC Sept. 4, 2008) 52

In re Proceedings Required by § 702(i) of the FAA,
No. 08-01, 2008 WL 9487946 (FISC Aug. 27, 2008) 7

Jerome B. Grubart, Inc. v. Great Lakes Dredge & Dock Co.,
513 U.S. 527 (1995) 24, 54

Jewel v. NSA,
673 F.3d 902 (9th Cir. 2011)..37

Kerns v. United States,
585 F.3d 187 (4th Cir. 2009)..23

Kowalski v. Turner,
543 U.S. 125 (2004) 61

Lucas v. S. Carolina Coastal Council,
505 U.S. 1003 (1992) 54

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 22

Maya v. Centex Corp.,
658 F.3d 1060 (9th Cir. 2011)..24

Monsanto v. Geertson Seed Farms,
561 U.S. 139 (2010) 55

Nat'l. Treasury Emps. Union v. Von Raab,
489 U.S. 656 (1989) 61

Owens v. Balt. City State's Attorney's Office,
767 F.3d 379 (4th Cir. 2014).. 23, 37, 41, 48

Phillips v. LCI Int'l, Inc.,
190 F.3d 609 (4th Cir. 1999)..44

S. Walk at Broadlands Homeowner Ass'n v. Openband at Broadlands, LLC,
713 F.3d 175 (4th Cir. 2013)..57

Schulz v. Pennsylvania R.R. Co.,
350 U.S. 523 (1956) 38

SD3, L.L.C. v. Black & Decker, Inc.,
801 F.3d 412 (4th Cir. 2015) .... passim

Sec'y of State v. Joseph H. Munson Co., Inc.,
467 U.S. 947 (1984) 58

Susan B. Anthony List v. Driehaus,
134 S. Ct. 2334 (2014) 22, 39, 54

Warth v. Seldin,
422 U.S. 490 (1975) 22

Zak v. Chelsea Therapeutics Int'l, Ltd.,
780 F.3d 597 (4th Cir. 2015) 23

Statutes

5 U.S.C. § 702 1

28 U.S.C. § 1291 1

28 U.S.C. § 1331 1

50 U.S.C. § 1801 .... 7, 9

50 U.S.C. § 1803 5

50 U.S.C. § 1804 5

50 U.S.C. § 1805 5

50 U.S.C. § 1809 5

50 U.S.C. § 1881a 7, 8, 9

Protect America Act, Pub. L. No. 110-55 (2007) 6

Other Authorities

Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*,
N.Y. Times, Aug. 8, 2013 44

David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* (July 2015) 14, 32

Final Report of the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, S. Rep. No. 94-755 (1976) 4

Hearing of the Privacy and Civil Liberties Oversight Board (July 9, 2013) 8

Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 46

Office of the Director of National Intelligence, 2014 Statistical Transparency Report (Apr. 22, 2015) 10, 43

PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (2014) .... passim

XKEYSCORE for Counter-CNE, *Intercept*, July 1, 2015 33

STATEMENT OF JURISDICTION

The district court had jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 5 U.S.C. § 702. That court entered a final order granting Defendants–Appellees' motion to dismiss on October 23, 2015. JA 204. Plaintiffs–Appellants timely filed a notice of appeal on December 15, 2015. JA 205. This Court has jurisdiction pursuant to 28 U.S.C. § 1291.

STATEMENT OF THE ISSUE

Whether Plaintiffs have plausibly alleged standing to challenge the National Security Agency's Upstream surveillance of their internet communications, given their detailed factual allegations about the operation of this surveillance and about the interception of Plaintiffs' communications.

STATEMENT OF THE CASE

I. Introduction

This lawsuit challenges the suspicionless seizure and searching of internet traffic by the National Security Agency ("NSA") on U.S. soil. As the government's own disclosures make clear, the NSA is searching through the *contents* of international internet communications for information relating to its surveillance targets. This surveillance dragnet, called "Upstream" surveillance, involves an unprecedented invasion of the privacy of countless Americans—including Plaintiffs—who communicate internationally. It is the digital analogue of having a government agent open every letter that comes through a mail processing center to read its contents before determining which letters to keep.

The government conducts Upstream surveillance by tapping directly into the internet "backbone" inside the United States with the compelled assistance of major telecommunications providers. Using surveillance equipment installed on the backbone—the high-capacity network that forms the heart of the internet—the NSA monitors circuits carrying Americans' domestic and international communications. In the course of this surveillance, the NSA seizes international text-based communications—and many domestic communications as well—and reviews the contents of these communications for tens of thousands of search terms. The surveillance exceeds the scope of the authority that Congress provided in the FISA Amendments Act of 2008 ("FAA") and violates the First and Fourth Amendments. Because it is predicated on programmatic surveillance orders issued by the Foreign Intelligence Surveillance Court ("FISC") in the absence of any case or controversy, the surveillance also violates Article III of the Constitution.

Plaintiffs collectively engage in more than a trillion sensitive international communications over the internet each year. Plaintiffs include the Wikimedia Foundation ("Wikimedia"), Human Rights Watch, the National Association of Criminal Defense Lawyers ("NACDL"), the Rutherford Institute, and other legal, human rights, and media organizations. Plaintiff Wikimedia operates one of the ten most-visited websites in the world and communicates with hundreds of millions of individuals who visit Wikipedia webpages to read or contribute to the vast repository of human knowledge that Wikimedia maintains online. The ability to exchange information in confidence, free from warrantless government monitoring, is essential to each of the Plaintiffs' work. The challenged surveillance violates Plaintiffs' privacy and undermines their ability to carry out activities crucial to their missions.

The district court held that Plaintiffs had failed to plausibly allege standing to challenge Upstream surveillance, but it reached this conclusion only by disregarding the detailed factual allegations in Plaintiffs' Amended Complaint and effectively reversing the presumptions that apply in assessing a motion to dismiss. Plaintiffs' allegations concerning how and why the government is surveilling their communications are supported by numerous government disclosures, extensive technological explanation, and credible news reports, including reports that describe or reproduce the NSA's documents. Plaintiffs have plausibly alleged that the government is copying and reviewing their communications in the course of Upstream surveillance. The court's dismissal of the Amended Complaint was in error.

II. Statutory Background

A. The Foreign Intelligence Surveillance Act of 1978

In 1975, Congress established a committee, chaired by Senator Frank Church, to investigate allegations of "substantial wrongdoing" by the intelligence agencies in their conduct of surveillance. Final Report of the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities (Book II), S. Rep. No. 94-755, at v (1976) ("Church Report"). The committee discovered that, over the course of decades, the intelligence agencies had "infringed the constitutional rights of American citizens" and "intentionally disregarded" legal limitations on surveillance in the name of "national security." *Id.* at 137. Of particular concern to the committee was that the agencies had "pursued a 'vacuum cleaner' approach to intelligence collection," in some cases intercepting Americans' communications under the pretext of targeting foreigners. *Id.* at 165. To ensure the protection of Americans' communications, the committee recommended that all surveillance of communications "to, from, or about an American without his consent" be subject to a judicial warrant procedure. *Id.* at 309.

In 1978, largely in response to the Church Report, Congress enacted FISA to regulate surveillance conducted for foreign intelligence purposes. The statute created the FISC and empowered it to review government applications for surveillance in certain foreign intelligence investigations. *See* 50 U.S.C. § 1803(a).

As originally enacted, FISA generally required the government to obtain an individualized order from the FISC before conducting electronic surveillance on U.S. soil. *See id.* §§ 1805, 1809(a)(1). To obtain a FISA order, the government was required to make a detailed factual showing with respect to both the target of the surveillance and the specific communications facility—such as a telephone line—to be monitored. *See id.* § 1804(a). The FISC could issue an order authorizing surveillance only if it found that, among other things, there was "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power," and "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2).

The basic framework established by FISA remains in effect today, but it has been gravely weakened by the FAA to permit the acquisition of U.S. persons' international communications without probable cause or individualized suspicion, as described below.[1]

[1] Throughout this brief, Plaintiffs use the phrase "U.S. persons" to refer to United States citizens and residents. Plaintiffs use the term "international" to describe communications that either originate or terminate outside the United States, but not both.

B. The Warrantless Wiretapping Program

On October 4, 2001, President George W. Bush secretly authorized the NSA to engage in warrantless electronic surveillance inside the United States. After *The New York Times* exposed the program and a federal district court ruled the program unconstitutional, *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), the government stated that it would seek authorization from the FISC. One FISC judge authorized the surveillance but another later found it unlawful. *See In re* [*Redacted*], No. [Redacted], at 13–16 (FISC Apr. 3, 2007) (Vinson, J.), http://1.usa.gov/1EljnuE. Subsequently, the government sought legislative amendments to FISA that granted authorities beyond what FISA had allowed for three decades.

C. The FISA Amendments Act of 2008

The legislative amendments sought by the Bush administration were embodied in the FAA.[2] The FAA radically revised the FISA regime by authorizing the government's warrantless acquisition of U.S. persons' international communications from companies inside the United States. Like FISA surveillance, FAA surveillance takes place on U.S. soil. However, surveillance under the FAA is far more sweeping than surveillance traditionally conducted under FISA, and the

---

[2] In August 2007, Congress passed a predecessor statute, the Protect America Act, Pub. L. No. 110-55, 121 Stat. 552 (2007), whose authorities expired in February 2008.

FAA's implications for U.S. persons' constitutional rights are correspondingly far-reaching.

First, unlike FISA, the FAA allows the government to warrantlessly monitor communications between people inside the United States and foreigners abroad. Specifically, it authorizes the government to intercept communications—including those of U.S. persons—when at least one party to a phone call or internet communication is a foreigner abroad targeted by intelligence officials. *See* 50 U.S.C. § 1881a(a) (authorizing "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information"). Importantly, surveillance conducted under the FAA may be conducted for many purposes, not just counterterrorism. The statute defines "foreign intelligence information" broadly to include, among other things, any information bearing on the foreign affairs of the United States. *Id.* § 1801(e).

Second, whereas surveillance under FISA is subject to individualized judicial authorization, surveillance under the FAA is not. To the contrary, the FISC's role in authorizing FAA surveillance is "narrowly circumscribed" by the statute, *In re Proceedings Required by § 702(i) of the FAA*, No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008), and consists principally of reviewing the general procedures the government proposes to use in carrying out its surveillance, *see* 50 U.S.C. § 1881a(i). Before obtaining an FAA order, the government must provide to the FISC a written certification attesting that the FISC has approved, or that the government has submitted to the FISC for approval, both "targeting procedures" and "minimization procedures." *Id.* § 1881a(d)–(g). These procedures dictate, at a high level of generality, who may be targeted for surveillance by the executive branch and how communications are to be handled once intercepted. The role that the FISC plays under the FAA bears no resemblance to the role it has traditionally played under FISA or the Fourth Amendment.[3]

Third, and relatedly, the FAA, unlike FISA, authorizes surveillance not predicated on probable cause. When the government submits an FAA application to the FISC, it need not demonstrate that its surveillance targets are agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Rather, the FAA permits the government to target *any* foreigner located outside the United States to obtain foreign intelligence information. Further, the FAA does not require the government to identify the specific "facilities, places, premises, or property at which" its surveillance will be directed. *Id.* § 1881a(g)(4). Thus, the government may direct its surveillance at major internet chokepoints, through which flow the communications of millions of people, rather than at

[3] *See, e.g.*, Hearing of the Privacy and Civil Liberties Oversight Board ("PCLOB") at 31:27–32:28 (July 9, 2013), http://cs.pn/177IpII (statement of former FISC Judge James Robertson).

individual telephone lines or email addresses.[4] Because the FAA requires neither particularity nor probable cause, the government can rely on a single FISC order to intercept the communications of countless individuals for up to a year at a time.

To the extent the statute provides safeguards for U.S. persons, the safeguards take the form of "minimization procedures." 50 U.S.C. §§ 1881a(e), 1801(h)(1). The statute's minimization requirements are supposed to protect against the collection, retention, and dissemination of communications that may be intercepted "incidentally" or "inadvertently." Significantly, however, these provisions include an exception that allows the government to retain communications—including those of U.S. persons—if the government concludes that they contain any information broadly considered "foreign intelligence." *Id.* §§ 1801(h), 1801(e). In other words, the statute allows the government to retain, analyze, and use U.S. persons' communications in investigations.

By dispensing with FISA's principal limitations, the FAA exposes every international communication—that is, every communication between an individual in the United States and a non-American abroad—to potential surveillance. And as discussed below, the government is using the statute to conduct precisely the kind

[4] PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* 36–37 (2014), http://bit.ly/1FJat9g ("PCLOB Report") (incorporated into the Amended Complaint by reference).

of vacuum-cleaner-style surveillance that the Church Committee condemned and that the Fourth Amendment was intended to prohibit.

III. Statement of the Facts

A. The Government's Implementation of the FISA Amendments Act

As Plaintiffs explain in their Amended Complaint ("Compl."), the government has implemented the FAA broadly, relying on the statute to intercept and retain huge volumes of Americans' communications. Compl. ¶ 37 (JA 39). In 2011, FAA surveillance resulted in the retention of more than 250 million communications—a number that does not reflect the far larger quantity of communications whose contents the NSA searched before discarding them. *Id.* ¶¶ 49–50, 62–63 (JA 43–44, 48–49).[5] In 2014, the government targeted the communications of 92,707 individuals, groups, and organizations under a single FISC order.[6] Every time a U.S. person communicates with any one of the government's targets—a target who may be a journalist, academic, or human rights researcher—his or her communications are intercepted and retained. The government refuses to disclose how many U.S. persons' communications it intercepts or retains under the FAA, but by all indications that number is staggering. *Id.* ¶ 37 (JA 39).

---

[5] *See* [*Redacted*], No. [Redacted], 2011 WL 10945618, at *9–10 (FISC Oct. 3, 2011); PCLOB Report 111 n.476.

[6] Compl. ¶ 37 (JA 39); Office of the Director of National Intelligence ("ODNI"), 2014 Statistical Transparency Report at 1 (Apr. 22, 2015), http://1.usa.gov/1JFUMll.

As required by the statute, the government has proposed targeting and minimization procedures and the FISC has approved them. Although these procedures are ostensibly meant to protect the privacy of U.S. persons, the procedures are weak and riddled with exceptions. By design, they give the government broad latitude to analyze and disseminate U.S. persons' communications—including using those communications in unrelated criminal investigations of Americans. *Id.* ¶¶ 52–54 (JA 45–46).

The government has acknowledged that it conducts two types of surveillance under the FAA. *See* PCLOB Report 7, 33–41. Under a program called "PRISM," the government obtains stored and real-time communications directly from U.S. companies—such as Google, Facebook, and Microsoft—that provide communications services to targeted accounts. This case concerns a second form of surveillance, called Upstream surveillance.

B. Upstream Surveillance

Upstream surveillance under the FAA involves the government's warrantless search and seizure of U.S. persons' internet communications as those communications transit networks on U.S. soil. Compl. ¶ 40 (JA 40). In the course of this surveillance, the NSA seizes Americans' communications in bulk and reviews the contents of substantially all international text-based communications—and many domestic communications as well—for tens of thousands of search terms. *Id.* at ¶ 48 (JA 43).

The government has disclosed a significant amount of information about Upstream surveillance. According to the government, Upstream surveillance entails the monitoring of communications as they travel across circuits on the internet "backbone" inside the United States. *See* PCLOB Report 35–37; Compl. ¶ 40 (JA 40); Def. Mot. Dismiss 10, ECF No. 77-1. The internet backbone is the network of high-capacity cables, switches, and routers that facilitates both domestic and international communication via the internet. *See* PCLOB Report 35–36; Compl. ¶¶ 41–47 (JA 40–43). When individuals engage in any kind of internet activity, such as browsing a webpage or sending an email, their communications are broken up into data "packets," which are transmitted separately across the internet backbone. Once these packets reach their destination, the recipients' computers reassemble the packets to reconstruct the communication. *See* PCLOB Report 125; Compl. ¶¶ 41–46, 66 (JA 40–42, 50).

The NSA conducts Upstream surveillance using surveillance devices installed on the internet backbone. Compl. ¶ 47 (JA 42–43). These surveillance devices are located strategically at chokepoints through which flow almost all internet communications entering or leaving the country. *Id.* ¶¶ 60, 68–69 (JA 47, 50–51). With the assistance of telecommunications providers, the NSA copies and reviews "text-based" communications—*i.e.*, those whose content includes searchable text, such as emails, search-engine queries, and webpages—for search terms, called "selectors." *Id.* ¶ 48 (JA 43). These selectors include email addresses, phone numbers, internet protocol ("IP") addresses, and other identifiers that NSA analysts believe to be associated with foreign intelligence targets. *Id.* ¶ 49 (JA 43–44).

Upstream surveillance encompasses the following processes, some of which are implemented by telecommunications providers at the NSA's direction:

- **Copying**. Using surveillance devices installed at key access points along the internet backbone, the NSA intercepts and makes a copy of *substantially all* international text-based communications—and many domestic ones—flowing across certain high-capacity cables, switches, and routers. *Id.*

- **Filtering**. The NSA attempts to filter out and discard some wholly domestic communications from the stream of internet data, while preserving international communications. The NSA's filtering out of domestic communications is incomplete, however—which means that many domestic communications are subject to warrantless surveillance. *Id.*; *see* PCLOB Report 38–41.

- **Content Review**. The NSA reviews the copied communications—including their full content—for instances of its search terms. Again, the search terms are email addresses, phone numbers, and other identifiers associated with the NSA's targets, but those targets need not be suspected terrorists or criminals—they may be journalists, academics, lawyers, or human rights researchers. Compl. ¶¶ 49, 36 (JA 43–44, 39).

- **Retention and Use**. The NSA retains all communications that contain selectors associated with its targets, as well as those that happened to be bundled with those communications in transit—totaling tens of millions of communications each year.[7] NSA analysts may read and query these communications with few restrictions, and they may share the results with the FBI, including in aid of criminal investigations. *Id.* ¶ 49 (JA 43–44).

One aspect of Upstream surveillance bears emphasis. Upstream surveillance is not limited to communications sent or received by the NSA's targets. The government has acknowledged that the NSA is engaging in what is called "about" surveillance, which involves systematically searching international internet traffic for any communications that contain "selectors" thought to be associated with the government's targets. *See* Compl. ¶¶ 49–50, 53, 62–66 (JA 43–45, 48–50); PCLOB Report 7, 37–38, 122. It has acknowledged, in other words, that the NSA intercepts vast quantities of internet traffic and examines the contents of essentially *everyone's* communications to determine whether they include references to the NSA's search terms. *See, e.g.*, PCLOB Report 111 n.476; *id.* at 37–38, 120 (acknowledging that the NSA "screens" communications transiting the internet backbone in search of its selectors); *see also* David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015) ("NSA's machines scan the contents of *all* of the communications passing through the collection point."). This is the digital analogue of having a government agent open every letter that comes through a mail processing center to determine whether it mentions a particular word or phrase. Although it could do so, the government

[7] [*Redacted*], 2011 WL 10945618, at *10 & n.26.

makes no meaningful effort to avoid the interception of communications that are merely "about" its targets (as opposed to those "to" or "from" its targets); nor does it later purge those communications. *See* PCLOB Report 122; Compl. ¶¶ 50–51 (JA 44–45).

C. Plaintiffs' Communications

Collectively, Plaintiffs—educational, legal, human rights, and media organizations—engage in an immense number of internet communications every single day, with individuals located in virtually every country on earth. Compl. ¶¶ 58, 61, 85, 88 (JA 46, 48, 55–56). Plaintiffs' work requires them to engage in sensitive and sometimes privileged communications, both international and domestic, with, among others, journalists, clients, experts, attorneys, foreign government officials, victims of human rights abuses, and individuals who are of investigative interest to the U.S. government. *Id.* ¶¶ 55, 104, 115, 125, 133, 138, 143, 148, 153, 158, 163 (JA 46, 61, 66, 69, 72–74, 76–81, 83).

As the operator of one of the most-visited websites in the world, Plaintiff Wikimedia alone engages in more than one trillion international internet communications each year. *Id.* ¶ 88 (JA 56). Wikimedia communicates with millions of individuals abroad who read, edit, and contribute to the twelve Wikimedia "Projects" from nearly every country on earth. *Id.* ¶¶ 6, 85, 88 (JA 31, 55–56). The best-known of Wikimedia's Projects is Wikipedia—a free internet encyclopedia that is one of the largest collections of shared knowledge in human history. In 2014, Wikipedia contained more than 33 million articles in over 275 languages, and collectively the Wikimedia sites received between approximately 412 and 495 million monthly visitors. *Id.* ¶ 79 (JA 53). Wikipedia's content is collaboratively researched and written by millions of volunteers, many of whom choose not to identify themselves, and is in most instances open to editing by anyone. *Id.*

Upstream surveillance implicates at least three categories of Wikimedia communications:

- **Communications of Wikimedia with its community members**. Wikimedia engages in more than one trillion international communications each year with those who read and contribute to Wikimedia's Projects and webpages, and with those who use the Projects and webpages to interact with each other. Many, but not all, of these communications are HTTP or HTTPS "requests" and "responses" required to view, search, log in, edit, or contribute to a Wikimedia webpage. *Id.* ¶ 88–92 (JA 56–58).

- **Wikimedia's internal "log" communications.** Wikimedia creates and transmits records related to its users' activities on its webpages in order to help it monitor, study, and improve the Projects. Every time Wikimedia receives a request from a person accessing a Project webpage, it creates a corresponding log entry. In May 2015, Wikimedia transmitted more than 140 billion logs from its servers abroad to its servers in the United States. *Id.* ¶ 93 (JA 58).

- **Communications of Wikimedia staff.** Wikimedia's staff communicate daily with individuals around the world in order to carry out the organization's mission. Their international contacts include foreign government officials, telecommunications companies, legal counsel, project partners, and volunteers. *Id.* ¶¶ 102, 104 (JA 61–62).

Wikimedia's communications are essential to its organizational mission, as is its ability to protect the privacy of these communications. *Id.* ¶ 89 (JA 57).

Because of the information they contain, Wikimedia's communications with its community members, as well as its internal communications related to the study and improvement of the Projects, are especially sensitive and private. *Id.* ¶ 95 (JA 59). They contain information indicating which specific webpages each particular Wikimedia community member is visiting or editing. *Id.* ¶¶ 89–91, 93 (JA 57–58). As a consequence, they provide a detailed picture of the everyday concerns of Wikimedia's users, and often constitute a record of their political, religious, sexual, medical, and expressive interests. *Id.* ¶ 95 (JA 59). Seizing and searching these communications is akin to seizing and searching the patron records of the largest library in the world.

As an organization, Wikimedia has an acute interest in the privacy of its communications. *Id.* ¶ 98 (JA 59–60). Wikimedia's communications reveal whom it exchanges information with—*i.e.*, who has contributed to the Projects or visited them—and they reveal exactly *what* information Wikimedia has exchanged with any individual user. *Id.* They reveal proprietary information about the use of Wikimedia's websites, which Wikimedia logs internally for its own purposes as part of its efforts to study and improve the Projects. *Id.* ¶ 93 (JA 58). They also reveal other private information about Wikimedia's operations, including details about its technical infrastructure, its data flows, and its member community writ large. *Id.* ¶ 99 (JA 60).

Wikimedia's mission and existence depend on its ability to ensure that readers and editors can explore and contribute to the Projects privately when they choose to do so. *Id.* ¶ 98 (JA 59–60). Except when editors publicly disclose their IP addresses, these exchanges are not public; they are private interactions between Wikimedia and its community members. *Id.* (Even when editors publicly disclose their IP addresses, some aspects of their exchanges remain private.) Wikimedia takes numerous, costly steps to protect the confidentiality of its communications. *Id.* ¶¶ 100–01 (JA 60–61). Doing so is vitally necessary to fostering trust with community members and to encouraging the growth, development, and distribution of free educational content. *Id.* ¶ 98 (JA 59–60).

IV. Procedural History

In March 2015, Plaintiffs filed suit against the NSA and other government defendants, challenging Upstream surveillance. Plaintiffs alleged that Upstream surveillance violates the First and Fourth Amendments and exceeds the scope of the authority that Congress provided in the FAA. In addition, Plaintiffs alleged that the surveillance violates Article III of the Constitution because it is predicated on programmatic surveillance orders issued by the FISC in the absence of any case or controversy. Plaintiffs amended their complaint as of right in June 2015. *See* Compl. (JA 27).

Defendants subsequently moved to dismiss Plaintiffs' Amended Complaint under Federal Rule of Civil Procedure 12(b)(1) for failure to plausibly allege Article III standing. *See* Def. Mot. Dismiss 2–3. The district court granted Defendants' motion to dismiss on October 23, 2015. Op. at 30 (JA 203). The court concluded that Plaintiffs' standing allegations were not plausible under *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). Op. at 27 (JA 200).

SUMMARY OF THE ARGUMENT

Plaintiffs have set forth detailed factual allegations describing the interception of their communications in the course of Upstream surveillance. Under well-established pleading standards, Plaintiffs have plausibly alleged standing to challenge this surveillance. The district court erred by failing to accept Plaintiffs' detailed and meticulously supported allegations as true, and by repeatedly drawing inferences *against* Plaintiffs.

Plaintiffs have demonstrated standing in two independent ways.

First, Plaintiff Wikimedia has plausibly alleged that, in the course of Upstream surveillance, the government is copying and reviewing at least some of its trillion or more annual communications. This is true for reasons explained at length in the Amended Complaint: (1) Wikimedia's communications traverse every major internet circuit entering or leaving the United States; and (2) as a technological matter, Upstream surveillance requires that the NSA copy and review all international text-based communications transiting the circuits it is monitoring, including Wikimedia's communications. In other words, even if the NSA were conducting Upstream surveillance on only a single circuit, it would be copying and reviewing the Wikimedia communications that traverse that circuit. But the government has acknowledged monitoring multiple internet circuits—making it only more certain that Wikimedia's communications are being copied and reviewed. Moreover, the NSA's own documents indicate that it is copying and reviewing Wikimedia's communications. Taken together, these detailed factual allegations leave no doubt as to the plausibility of Wikimedia's standing.

Second, all of the Plaintiffs have plausibly alleged that the NSA is copying and reviewing substantially all text-based communications entering and leaving the United States, including their own. This allegation follows necessarily from the information the government has officially disclosed, and it is corroborated by independent news reports. As the Amended Complaint explains, for Upstream surveillance to serve the purposes the government has said it serves, the NSA must be comprehensively monitoring text-based communications originating or terminating in the United States. Internet communications take inherently unpredictable paths across the internet backbone, and so to reliably intercept communications to, from, and about thousands of targets around the globe, the NSA must monitor substantially all international communications, including those of Plaintiffs. And, in fact, the NSA's own documents show that it is monitoring many of the backbone chokepoints through which the vast majority of internet traffic enters and leaves the country.

The district court erred in holding that *Clapper v. Amnesty International USA* forecloses Plaintiffs' standing. *Amnesty* involved a challenge to a different form of surveillance by plaintiffs who could not establish that the surveillance they complained of was taking place, or that their own communications would be subject to it. This case, by contrast, involves a challenge to a different—and far broader—form of surveillance, by plaintiffs who, because of unprecedented government disclosures, as well as the volume and dispersion of their own communications, have plausibly alleged that the surveillance they complain of is taking place and that their own communications are already subject to it. The district court acknowledged some of the differences between Plaintiffs' suit and *Amnesty*, but it failed to recognize their significance. In short, Plaintiffs here have pleaded directly what the plaintiffs in *Amnesty* could only speculate about: that the NSA is intercepting their communications. That allegation is well-pled and plausible. The district court erred in concluding otherwise.

STANDARD OF REVIEW

Where a defendant has challenged the legal sufficiency of the complaint on its face pursuant to Rule 12(b)(1), this Court reviews *de novo* the district court's dismissal for lack of subject-matter jurisdiction. *Columbia Gas Transmission Corp. v. Drain*, 237 F.3d 366, 369 (4th Cir. 2001).

ARGUMENT

I. The district court erred in holding that Plaintiffs had not plausibly alleged the copying and review of their communications.

A. Legal standards.

To establish standing, a complaint must include factual allegations that, accepted as true, demonstrate: (1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision. *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). The injury-in-fact requirement is designed to ensure that the plaintiff has a "personal stake in the outcome of the controversy." *Warth v. Seldin*, 422 U.S. 490, 498 (1975). The asserted injury must be "'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Susan B. Anthony List*, 134 S. Ct. at 2341 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). Importantly, a plaintiff seeking prospective relief need allege only a "substantial risk"—not a certainty—of harm. *See id.* (quoting *Amnesty*, 133 S. Ct. at 1150 n.5).

Where a defendant raises a "facial" challenge to a complaint under Rule 12(b)(1)—as the government does here, *see* Op. at 10 n.8 (JA 183)—a court must determine whether the complaint contains "sufficient factual matter, accepted as true" to "'state a claim [to standing] that is *plausible* on its face.'" *Iqbal*, 556 U.S. at 678) (emphasis added); *see Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982). Because a complaint's "plausibility" turns on the sufficiency of the pleadings, a court must limit its inquiry to the four corners of the complaint and to any documents incorporated by reference. *See Zak v. Chelsea Therapeutics Int'l, Ltd.*, 780 F.3d 597, 606–07 (4th Cir. 2015). In addition, factual allegations that are specific and detailed must be taken as true, and all reasonable inferences must be drawn in favor of the plaintiff. *See Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009); *Cooksey v. Futrell*, 721 F.3d 226, 234 (4th Cir. 2013). The Fourth Circuit has emphasized that a complaint is "plausible" and "should not be dismissed as long as it provides sufficient detail about the claim to show that the plaintiff has a more-than-conceivable chance of success on the merits." *Goldfarb v. Mayor & City Council of Balt.*, 791 F.3d 500, 511 (4th Cir. 2015); *see Owens v. Balt. City State's Attorney's Office*, 767 F.3d 379, 403 (4th Cir. 2014) ("The recitation of facts need not be particularly detailed, and the chance of success need not be particularly high."). Importantly, the plausibility standard is not an invitation for courts to weigh the *probability* of competing explanations. Thus, a court cannot substitute its own "perception of the relevant events over the narrative offered by the complaint." *SD3, L.L.C. v. Black & Decker, Inc.*, 801 F.3d 412, 430–31 (4th Cir. 2015); *see Houck v. Substitute Tr. Servs., Inc.*, 791 F.3d 473, 484 (4th Cir. 2015). Rather, a court must credit the plaintiff's factual allegations and, on that basis, determine whether the complaint shows more than the "sheer possibility" that the plaintiff has standing. *Iqbal*, 556 U.S. at 678.[8]

As explained below, Plaintiffs have plausibly alleged standing here.

B. Wikimedia has plausibly alleged that the government is copying and reviewing at least some of its trillion or more international communications.

Wikimedia has plausibly alleged that, in the course of Upstream surveillance, the government is copying and reviewing at least some of its trillion or more annual communications. This is true for two reasons: (1) Wikimedia's communications traverse every major internet circuit entering or leaving the United States; and (2) as a technological matter, Upstream surveillance requires that the NSA copy and review *all* international text-based traffic on the circuits it is monitoring, including Wikimedia's communications.

---

[8] It is an open question whether *Iqbal*'s plausibility requirement, as opposed to a lower threshold, applies to a motion to dismiss under Rule 12(b)(1). *See Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011); *Jerome B. Grubart, Inc. v. Great Lakes Dredge & Dock Co.*, 513 U.S. 527, 537–38 (1995). The answer is immaterial here because Plaintiffs' allegations plainly meet the plausibility threshold.

Thus, as Wikimedia explains in detail, the NSA could not conduct Upstream surveillance—as the government itself has described it—without copying and reviewing Wikimedia's communications. Because of the basic rules governing communication on the internet, and because Wikimedia has hundreds of millions of users distributed around the globe, Wikimedia's international communications are unavoidable as the NSA monitors traffic entering and leaving the United States. Wikimedia is prepared to prove its allegations through, among other things, the testimony of technical experts; but on a motion to dismiss the district court was obliged to accept Wikimedia's non-conclusory, factual allegations as true.

1. Wikimedia's communications traverse every major internet circuit entering or leaving the United States.

As the operator of one of the ten most-visited websites in the world, Wikimedia engages in more than a trillion international internet communications each year. Compl. ¶ 88 (JA 56). Wikimedia's hundreds of millions of users are located in virtually every country on earth and communicate with Wikimedia from hundreds of millions of locations on the internet. *Id.* ¶ 85 (JA 55). Because Wikimedia's trillion-plus communications are so numerous and so widely distributed across the internet, its communications traverse every major internet circuit entering or leaving the United States. *Id.* ¶ 61 (JA 48).

That Wikimedia's communications flow across each of the major internet circuits is a function of not only Wikimedia's widely distributed global user community and the immense volume of Wikimedia's communications, but also the basic structure of the internet backbone. There are only a limited number of routes into and out of the United States, principally via the high-capacity circuits that connect major U.S. telecommunications providers with providers abroad. *See id.* ¶¶ 45–46, 60–62 (JA 42, 47–48); *see also* PCLOB Report 36–37.[9] Indeed, the junctions where these international circuits meet the domestic backbone are known as chokepoints precisely because almost all international internet traffic flows through the circuits that converge there. Compl. ¶¶ 60, 68–69 (JA 47–48, 50–51). As Wikimedia exchanges more than one trillion communications each year with users scattered across the global network, its communications are routed across every one of the major internet circuits connecting the United States with the rest of the world.

The government has acknowledged that it conducts Upstream surveillance on these major internet circuits. In particular, according to the FISC and the PCLOB, the NSA conducts its surveillance at more than one such "circuit" or "international Internet link" on the internet backbone. PCLOB Report 36–37; [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011); *see* Compl. ¶¶ 68–69

---

[9] These major internet circuits are carried on the approximately 49 international submarine cables—and limited number of high-capacity terrestrial cables—that transport the vast majority of internet traffic into and out of the United States. Compl. ¶ 60 (JA 47–48).

(JA 50–51). For the reasons above, Wikimedia's communications traverse each of these major internet circuits.

2. As a technological matter, the NSA must copy and review all international text-based communications transiting each of the circuits it monitors.

Not only do Wikimedia's communications traverse the major internet circuits that the NSA is monitoring, but the government could not conduct Upstream surveillance on the terms it has publicly disclosed without copying and reviewing at least some of Wikimedia's communications. That is because, as a technological matter, the NSA could not carry out the surveillance it has acknowledged conducting *except* by copying and reviewing all of the international text-based communications that travel across the individual circuits that it monitors. Compl. ¶¶ 62–63 (JA 48–49). Thus, the government would be copying and reviewing Wikimedia's communications even if it were monitoring only a single circuit.

As discussed above, the NSA has acknowledged that Upstream surveillance involves an exceptionally broad and novel form of surveillance: so-called "about" surveillance. That is, the NSA uses Upstream surveillance to search for communications "about" its thousands of targets, not just those to or from its targets. *Id.* ¶ 50 (JA 44). As the PCLOB observed, this is a defining feature of Upstream surveillance—one that raises unprecedented constitutional questions because it requires the NSA to systematically examine the *contents of non-targets' communications*. *See* PCLOB Report 121–22 ("[N]othing akin to 'about' collection could feasibly occur with respect to [] traditional forms of communication."). Under Upstream, the NSA reviews the contents of internet communications, like emails and webpages, looking for any that mention a targeted selector anywhere within them. Compl. ¶¶ 49–50 (JA 43–44); PCLOB Report 120; [*Redacted*], 2011 WL 10945618, at *11.

The NSA could not conduct "about" surveillance without copying and reviewing *all* of the international text-based communications on each circuit it is monitoring. Compl. ¶¶ 62–63 (JA 48–49). There is no other way, technologically, for the NSA to identify the communications it seeks. *Id.*; *see also id.* ¶¶ 41–46 (JA 40–42) (describing the rules and processes governing communication on the internet). The communications the NSA is looking for—those containing any one of the NSA's thousands of targeted selectors—are intermingled with the communications of everyone else that flow across the same circuit. Not only that, but individual communications are split up into smaller "packets" to enable their transmission across the internet, and those packets travel independently of one another, intermingled with packets of other communications on the same circuits. *Id.* ¶¶ 42, 63 (JA 41, 48–49); *see also* PCLOB Report 125. Because the communications are split into fragments while in transit, it is impossible to reliably obtain the communications of interest without first copying all of the international text-based packets on a given circuit, and then reassembling each individual communication. Compl. ¶ 63 (JA 48–49). Moreover, once the communications have been copied and reassembled, the NSA must still search the contents of each one, because it is impossible for the agency to know in advance which communications will contain a selector associated with one of its many moving targets. Compl. ¶ 62 (JA 48).[10] In other words, only by copying *all* international text-based packets on a circuit can the NSA ensure that it obtains the constituent pieces of any individual communication. And only by reviewing the contents of *all* the reassembled communications can the NSA ensure that it identifies those containing any one of its thousands of selectors. *Id.* ¶¶ 62–63 (JA 48–49).

The government's own disclosures corroborate Plaintiffs' explanation of how and why the NSA is copying and reviewing all international text-based communications on the circuits it monitors. For instance, the FISC has explained that the NSA's Upstream surveillance devices retain "*any* Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it." [*Redacted*], 2011 WL 10945618, at *11 (emphasis added). The PCLOB has

[10] The government admits this when it says that it "screens" internet communications in order to identify the subset that contain a targeted selector, *see* PCLOB Report 37, and that this process requires "access to a larger body of international communications than those that contain a tasked selector," *id.* at 111 n.476.

described the breadth of Upstream surveillance—as compared to traditional forms of surveillance—in similar terms. PCLOB Report 122 (analyzing the privacy implications of Upstream surveillance based on the government's use of technology that allows it "to examine the contents of *all* transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them") (emphasis added).[11] There is simply no technological shortcut that would allow the NSA to conduct the surveillance it has described without taking the steps Plaintiffs set out above. The NSA must copy, then reassemble, and then review all of the international text-based communications on a given internet circuit in order to determine which ones it wishes to retain. Compl. ¶¶ 42, 62–64 (JA 41, 48–49).

In sum, for every circuit that the NSA monitors, that monitoring must be comprehensive for the government to conduct Upstream surveillance as it has been publicly described. And because Wikimedia's communications traverse every

[11] The district court incorrectly hypothesized that simply because the NSA has the "capacity" to examine all international text-based communications passing through its collection devices, it was not necessarily engaging that capacity at "full throttle." Op. at 17–18 (JA 190–91). This hypothesis misunderstands the technology (as explained above), and it is belied by the FISC's and the PCLOB's analyses, which address Upstream surveillance as it *actually* operates. [*Redacted*], 2011 WL 10945618, at *11; PCLOB Report 120–22. At bottom, the district court improperly credited its own conjecture over Plaintiffs' detailed factual allegations explaining how and why Upstream surveillance entails the copying and review of communications in bulk. *See SD3*, 801 F.3d at 425.

major internet circuit into and out of the United States, the NSA is necessarily copying and reviewing Wikimedia's communications in the course of Upstream surveillance. Indeed, even if the NSA were conducting Upstream surveillance on only a *single* circuit, it would be copying and reviewing at least those Wikimedia communications that traverse that link. *Id.* ¶ 64 (JA 49).

The district court dismissed or misunderstood these detailed allegations. It certainly did not credit them as true, as it was required to do on a motion to dismiss; and it repeatedly drew inferences *against* Wikimedia rather than drawing all reasonable inferences in its favor. *See* Op. at 16–28 (JA 189–201).

First, the district court misunderstood the very nature and scope of "about" surveillance. *See* Compl. ¶¶ 50–51 (JA 44–45); PCLOB Report 37–38, 120–22. In particular, it suggested that "about" surveillance is not as broad as Plaintiffs allege because the surveillance is "targeted insofar as it makes use of only those communications that contain information matching the tasked selectors." Op. at 20 (JA 193). This ignores, however, the fact that the NSA must first search the contents of transiting communications before it can identify the subset that contain selectors. The government's own review board has acknowledged this fact, saying that Upstream surveillance requires the NSA to copy and review a far "larger body of international communications," to find the ones that contain the keywords it is searching for. PCLOB Report 111 n.476. As Plaintiffs explain, the NSA must search, at a minimum, all international text-based communications on each circuit it is monitoring. Compl. ¶¶ 50, 62–64 (JA 44, 48–49); *see also* Kris & Wilson § 17.5. The district court's error suggests that it misunderstood the very nature of the surveillance challenged in this lawsuit. The significance of this error cannot be overstated, because the scope of Upstream surveillance is critical both to Plaintiffs' standing and to the merits of this case. In carrying out Upstream surveillance, the NSA is seizing and searching essentially everyone's communications on a given circuit—targets and non-targets alike—in order to discover which communications it wants to retain for later use.

Second, the district court simply rejected outright Plaintiffs' detailed explanation of why, as a technological matter, the NSA must copy and review all the international text-based communications on the circuits it is monitoring. Op. at 26 (JA 199). The district court was required to credit Plaintiffs' factual allegations, *see Cooksey*, 721 F.3d at 234, but instead it rejected wholesale Plaintiffs' account of these processes, as though the NSA were impervious to inferences and conclusions grounded in scientific and technological principles. It is as if the district court held that Plaintiffs could only speculate about whether the laws of physics apply to the NSA. Plaintiffs are prepared to prove their allegations through, among other things, the testimony of technical experts; but on a motion to dismiss the district court was obliged to accept Plaintiffs' factual allegations as true.

3. For additional reasons, it is clear that the NSA is copying and reviewing at least some of Wikimedia's trillion-plus international communications.

There are several additional reasons to conclude that Wikimedia's allegations about the copying and review of its communications are plainly plausible.

First, the NSA's own documents indicate that it is copying and reviewing Wikimedia's communications in order to obtain intelligence information. Compl. ¶ 107 (JA 63). One NSA slide describes analysts' ability to learn "nearly everything a typical user does on the Internet" by surveilling HTTP communications—and identifies Wikipedia traffic as a target for this kind of surveillance. *Id.* The slide pertains to a search tool that allows NSA analysts to examine data intercepted via Upstream surveillance. *See id.*[12]

[12] Another NSA document, which was published in the press only after the Amended Complaint was filed, similarly confirms that the NSA is intercepting Wikimedia's communications. *See* XKEYSCORE for Counter-CNE, *Intercept*, July 1, 2015, http://bit.ly/1Jr79Uc (Slide 9). This document shows that the NSA has designed its search software to allow analysts to identify intercepted Wikimedia communications, including those retained in the course of Upstream surveillance. *Id.* (describing computer code that identifies "wikimedia" and "wikipedia" HTTP communications).

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Why are we interested in HTTP?
facebook
YAHOO!
twitter
myspace.com
a place for friends
Because nearly everything a typical user does on the Internet uses HTTP
CNN.com
Google
Earth
WIKIPEDIA
The Free Encyclopedia
Gmail
@mail.ru

If there were any doubt that the NSA is copying and reviewing Wikimedia's communications as it monitors international internet traffic, these NSA documents go even further: they show that the NSA is deliberately directing its analysts to intercepted Wikimedia communications as a specific source of intelligence.

Second, the NSA is conducting Upstream surveillance on many internet circuits—a fact that makes it only more certain that Wikimedia's communications are copied and reviewed. While Wikimedia would have standing even if the NSA were monitoring only a single major internet circuit—because Wikimedia's communications transit each one—the government is in fact monitoring many such circuits. *See* Compl. ¶¶ 65–66 (JA 49–50). This allegation is corroborated by NSA documents cited in the Amended Complaint. *Id.* ¶¶ 68–69 (JA 50–51) (showing that the NSA is conducting Upstream surveillance "at many of the chokepoints operated by U.S. providers"). Because the government's thousands of targets are scattered around the world, and because the paths their communications take into and out of the United States will often be in flux, Upstream surveillance could not be remotely effective *without* monitoring many major internet circuits. *See infra* Section I.C.1; Compl. ¶¶ 65–66 (JA 50).

When the breadth of the NSA's surveillance program is set alongside the immense volume of Wikimedia's communications, the plausibility of Wikimedia's allegations cannot be seriously disputed. The government's position is that Wikimedia's claim is implausible because it is conceivable the NSA is not copying and reviewing *any* of Wikimedia's more than one trillion international communications. *See* Def. Mot. Dismiss 23, 28–29. But if anything is implausible, it is the government's theory. Using a simple model, the Amended Complaint illustrates how difficult it would be for the NSA to avoid intercepting *every single one* of Wikimedia's communications. Compl. ¶¶ 58–59 (JA 46–47). In particular, as Plaintiffs have just explained, Upstream surveillance could achieve the government's purposes only if it entailed the copying and review of a large percentage of international text-based traffic. *See also id.* ¶¶ 65–66 (JA 49–50).

But even if one were to make the extremely conservative assumption that there is as little as a 0.00000001% chance the NSA will copy and review any particular internet communication, the odds of the government copying and reviewing at least one of Wikimedia's communications in a one-year period would still be greater than 99.9999999999%. *Id.* ¶ 58 (JA 46–47).

The district court mistook this statistical illustration for Wikimedia's principal theory of standing—but it also misunderstood the illustration itself. *See* Op. at 24–25 (JA 197–98). The district court suggested that Wikimedia had simply picked a convenient percentage out of thin air, but in fact, it was chosen specifically to show what an incomprehensibly small sliver of internet communications the NSA could be surveilling and *still* be virtually certain to copy and review at least one of Wikimedia's communications. And, contrary to the district court's opinion, the Amended Complaint explains why the illustration's assumptions are exceedingly conservative and why the NSA is in fact far more likely to copy and review Wikimedia's communications than even this simple model shows.[13]

---

[13] In particular, Plaintiffs explain how and why Upstream surveillance is designed to sweep up precisely the kinds of international text-based communications that Wikimedia engages in on a massive scale. Compl. ¶¶ 59, 62–66 (JA 47–50); *see supra* Sections I.B.2–3.

The important point is that, even accounting for the assumptions embedded in it, the model shows how unlikely it is that the government's Upstream surveillance does not touch any of Wikimedia's communications. The model shows that, even if one makes extremely conservative assumptions about the scale of the government's surveillance, it is virtually certain—and surely plausible—that the surveillance implicates at least *some* of Wikimedia's trillion or more communications each year.

4. Wikimedia's standing allegations are plausible.

Given the wealth of support set out in the Amended Complaint, Wikimedia's allegations are plainly plausible. Indeed, to hold that a party that has alleged injury with reference to official disclosures, detailed technological explanation, news reports, and published government documents has not satisfied the "plausibility" standard requires a profound distortion of the pleading requirements. Neither *Iqbal* nor *Twombly* purported to turn those requirements into insuperable hurdles, and the courts have not interpreted these cases in the way that the district court did here. *See Owens*, 767 F.3d at 396, 403–04; *Jewel v. NSA*, 673 F.3d 902, 908–10 (9th Cir. 2011) (finding plaintiffs had standing, on a motion to dismiss, to challenge warrantless surveillance of their internet communications).

The district court cited *Iqbal* and *Twombly* in rejecting Plaintiffs' detailed factual allegations, but it did not apply the notice-pleading framework set out in those cases: it did not accept Plaintiffs' factual allegations as true, draw all reasonable inferences in Plaintiffs' favor, and then ask whether there was "more than a sheer possibility" that the NSA is copying and reviewing Plaintiffs' communications in the manner alleged. *Iqbal*, 556 U.S. at 678. It applied a far higher standard, refusing to credit *any* factual inference—even those based on the extensive public information about the breadth, operation, and purposes of Upstream surveillance. *Iqbal* and *Twombly* permit a court to disregard "conclusory" allegations—*i.e.*, legal conclusions masquerading as factual assertions. *See id.* But there is nothing conclusory about Wikimedia's explanation of how and why the government is monitoring its communications in the course of Upstream surveillance.

The district court apparently believed that because Plaintiffs do not have direct access to every detail about Upstream surveillance, any claim concerning the surveillance of their communications is fatally "speculative." *See* Op. at 27 (JA 200). But this is a standard of proof that does not apply even at trial, let alone on a motion to dismiss. Parties routinely rely on deduction, reasonable inference, and expert opinion to establish facts necessary to their claims. *See Schulz v. Pennsylvania R.R. Co.*, 350 U.S. 523, 526 (1956). Moreover, the motion-to-dismiss standard explicitly commands courts to draw all reasonable inferences in favor of the plaintiff, not least because the plaintiff will not yet have had a chance to develop the factual record fully at that early stage of the case. *See Susan B. Anthony List*, 134 S. Ct. at 2342 ("[E]ach element must be supported . . . with the manner and degree of evidence required at the successive stages of the litigation."); *SD3*, 801 F.3d at 434 (cautioning courts against "mistakenly collaps[ing] discovery, summary judgment, and trial into the pleading stages of a case").

Finally, and relatedly, the district court repeatedly characterized Wikimedia's standing claim as one premised on "probabilities," when it is not. *See, e.g.*, Op. at 23 (JA 196). Indeed, to the extent the district court engaged Wikimedia's specific allegations, it focused almost exclusively on Wikimedia's statistical illustration, while ignoring the technological explanation above. *See supra* Sections I.B.1–2. Although the statistical illustration reinforces the plausibility of Wikimedia's claims, Wikimedia's standing does not depend on that illustration. Wikimedia has standing because its communications flow across every major internet circuit entering or leaving the country, and the NSA could not, as a technological matter, implement the surveillance it has acknowledged except by copying and reviewing all of the international text-based traffic on the circuits it is monitoring—including Wikimedia's communications.

C. Plaintiffs have also plausibly alleged that the NSA is copying and reviewing "substantially all" international text-based communications, including their own.

For the reasons discussed above, Wikimedia would have standing even if the NSA were monitoring only a single major internet circuit. The Amended Complaint alleges, however, that the NSA's surveillance activities are broader. All of the Plaintiffs have standing to challenge Upstream surveillance because, as explained in the Amended Complaint, the NSA is copying and reviewing *substantially all* text-based communications originating or terminating in the United States, including the communications of Plaintiffs. Compl. ¶¶ 1, 47–50, 56, 69 (JA 30, 42–44, 46, 51).

This allegation follows necessarily from the information the government has officially disclosed, and it is corroborated by independent news reports. As discussed below, for Upstream surveillance to serve the purposes the government has said it serves, the NSA must be comprehensively monitoring text-based communications originating or terminating in the United States. This is the only way for the NSA to reliably obtain communications to, from, and about its thousands of targets around the world, because those communications travel along paths in and out of the country that are unpredictable and change over time. Moreover, the structure of the internet backbone facilitates such comprehensive surveillance. Because international communications are channeled through a small number of internet chokepoints—and because the NSA's own documents show that it is conducting Upstream surveillance at many of those chokepoints—it is straightforward for the government to conduct the comprehensive surveillance necessary for Upstream to function as described. The district court either failed to engage with or failed to credit Plaintiffs' allegations about the scope of Upstream surveillance, but these detailed and non-conclusory allegations are entitled to a presumption of truth at the pleading stage. *See Owens*, 767 F.3d at 385, 388.

1. The unpredictable routing of internet traffic requires comprehensive surveillance of international communications for Upstream surveillance to operate as the government has described.

The government's descriptions of Upstream surveillance make clear that the government is interested in obtaining, with a high degree of confidence, all international communications to, from, and about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to *comprehensively* acquire communications that are sent to or from its targets." PCLOB Report 10 (emphasis added). And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id*. at 143 (emphasis added).

Because the routing of internet traffic is unpredictable, however, the government can only "comprehensively" and "reliably" obtain communications to, from, and about its thousands of targets by conducting its surveillance on the different routes by which internet communications enter and leave the country, and by examining substantially all international communications that travel those various routes. As discussed below, that is precisely how the NSA is conducting Upstream surveillance.

The path that an internet communication takes is inherently unpredictable. Internet communications are routed around the globe based on a complex set of rules and relationships that are applied dynamically, based on network conditions at any given moment. *See* Compl. ¶¶ 42, 44–45 (JA 41–42). These network conditions change frequently, and so one cannot know in advance which path a particular communication will travel. Indeed, even the communications between two individuals in a single conversation (such as an internet chat or email exchange) may take entirely different routes across the internet backbone, even though the end-points are the same. For example, if an NSA target is having an internet chat conversation with someone in the United States, the communications *from* the target will frequently follow a different path than those *to* the target. And, of course, a target's location may vary over time. For all these reasons, a target's communications may traverse one internet circuit at one moment, but a different one later.

The fact that the NSA had, at last public count, 92,707 surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) only reinforces the conclusion that Upstream surveillance of international text-based communications is comprehensive. Compl. ¶¶ 37, 65–66 (JA 39, 49–50); *see* ODNI, 2014 Statistical Transparency Report at 1 (Apr. 22, 2015), http://1.usa.gov/1JFUMll. The communications of so many targets scattered around the world will travel many different routes across the internet backbone, based on the locations of those various targets, their individual movements over time, and changes in network conditions. Compl. ¶ 66 (JA 50). These communications will be intermingled with those of the general population in the flow of internet traffic. *Id.* ¶¶ 62–63 (JA 48–49). An intelligence agency that seeks to reliably intercept communications to, from, or about its targets, could do so only by searching substantially all text-based communications entering or leaving the country.

This allegation is based on the government's official disclosures and on necessary inferences from those disclosures, but it is also corroborated by news accounts. A *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A.

is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Compl. ¶ 69 (JA 51) (quoting Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi). The same *New York Times* report also explains, consistently with the Amended Complaint, why the NSA's Upstream surveillance is so far-reaching:

> Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data; fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled.

Compare id., *with* Compl. ¶¶ 62–63 (JA 48–49); *see Phillips v. LCI Int'l, Inc.*, 190 F.3d 609, 618 (4th Cir. 1999) (on a motion to dismiss, a court may consider newspaper articles that are "integral to and explicitly relied on in the complaint").[14]

---

[14] The district court dismissed the accuracy of this *New York Times* article, Op. at 18 n.16 (JA 191), but only based on a mistaken understanding of the PCLOB Report. The PCLOB Report says nothing that undermines the article's central claim that Upstream surveillance involves the "copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." *See* PCLOB Report 122, 111 n.476. The PCLOB Report took issue only with a smaller point: the article's suggestion that the NSA was looking for people "discussing particular subjects or using particular key words." The Report clarified that the NSA searches communications for "selectors," which are specific types of keywords (such as email addresses or phone numbers). *Id.* at 119.

2. The structure of the internet backbone facilitates comprehensive surveillance of Americans' international communications.

Not only does the NSA have an overriding incentive to copy and review substantially all international internet communications, but the internet backbone is structured in a way that enables it to do so.

The internet backbone funnels almost all internet communications entering and leaving the country through a limited number of chokepoints. As the Amended Complaint describes, the internet backbone includes approximately 49 international submarine cables (and a limited number of terrestrial cables) that transport internet traffic into and out of the United States. Compl. ¶¶ 46, 60 (JA 42, 47). Because there are relatively few high-capacity cables carrying international internet communications, there are correspondingly few chokepoints—*i.e.*, junctions through which all international internet communications must pass en route to their destinations. *Id.* By installing its surveillance equipment at the small number of backbone chokepoints, the NSA is able to monitor substantially all text-based communications entering or leaving the United States.[15]

Plaintiffs' Amended Complaint cites NSA documents published in the press that corroborate their allegation that the NSA has installed surveillance equipment

[15] As noted above, the government has acknowledged that it conducts Upstream surveillance at international links and on the internet backbone. [*Redacted*], 2011 WL 10945618, at *15; PCLOB Report 36–37.

at many major chokepoints on the internet backbone. Compl. ¶¶ 68–69 (JA 50–51). One of these NSA documents states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *Id.* ¶ 69 (JA 51). Another shows that just one of those participating providers has facilitated Upstream surveillance at seven major international chokepoints in the United States. *Id.* ¶ 68 (JA 50–51).[16]

3. Plaintiffs' allegations that the NSA is intercepting substantially all international text-based communications are plausible.

Despite these extensive allegations and corroborating reports from the government and others, the district court concluded that Plaintiffs had provided "no factual basis" to support the conclusion that the NSA is copying and reviewing substantially all text-based communications entering or leaving the United States. Op. at 18 (JA 191). For the reasons just explained, that conclusion is belied by the Amended Complaint. The district court simply declined to credit Plaintiffs' detailed explanation about why comprehensive monitoring of international text-based communications is not only feasible but operationally required in order for the NSA to carry out Upstream surveillance. *See supra* Sections I.C.1–2. Instead, the district court improperly credited its own hypothesis about the scope of Upstream surveillance, speculating that the FISC had imposed undisclosed limits on the NSA's surveillance. Op. at 18 (JA 191).[17] At the same time, the court dismissed the notion that the NSA's "strong incentive" to engage in such far-reaching surveillance supported the plausibility of Plaintiffs' standing claim. *Id.* But the Fourth Circuit has made clear that motivation matters when assessing plausibility. *SD3*, 801 F.3d at 431 (identifying motivation as "a key circumstantial fact"). Moreover, Plaintiffs' allegations do not rest on a general assertion that the NSA is motivated to collect intelligence; instead, Plaintiffs have explained in detail why, in order to operate as the government has described, Upstream surveillance *must* involve the copying and review of substantially all text-based international communications. Plaintiffs' allegations are borne out by the corroborating information cited in the Amended Complaint, including reporting by the *New York Times*, the opinions of computer scientists, and the NSA's own documents—all of which the district court disregarded.

---

[16] Additional reporting after the filing of the Amended Complaint states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015, http://nyti.ms/1NiJLY3.

[17] The district court reasoned that the mere existence of FISC review was itself proof that the NSA "is not using its surveillance equipment to its full potential." Op. at 18 (JA 191). But the FISC's opinions support Plaintiffs' allegations: they place no limitations whatsoever on the NSA's copying and review of Americans' *international* communications. *See, e.g.*, [*Redacted*], 2011 WL 10945618.

The district court was wrong to do so. As discussed above, the court should have taken as true all of Plaintiffs' non-conclusory allegations, and should have drawn all reasonable inferences in Plaintiffs' favor. *See Owens*, 767 F.3d at 396 (complaint should not be dismissed as long as it contains sufficient facts to show that the plaintiff "has a more-than-conceivable chance of success on the merits"); *SD3*, 801 F.3d at 430–31 ("[B]y favoring its perception of the relevant events over the narrative offered by the complaint, the dissent makes the very mistake that the district court made, recasting 'plausibility' into 'probability.'"); *Houck*, 791 F.3d at 484 ("The district court's inquiry into whether an alternative explanation was more probable undermined the well-established plausibility standard.").

* * *

Plaintiffs have alleged in detail the "who, what, when, and where" of Upstream surveillance in their Amended Complaint, and they have explained "why" this surveillance is as broad as it is. *SD3*, 801 F.3d at 431. Plaintiffs have made this showing on the basis of extensive government disclosures, a detailed description of the structure of the internet, credible news reports, and NSA documents published in the press. These allegations plausibly establish that the NSA is copying and reviewing Plaintiffs' communications in the course of Upstream surveillance.

II. The district court erred in holding that *Amnesty International USA* forecloses Plaintiffs' standing.

The district court was wrong to conclude that this case is controlled by *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). *See* Op. at 28 (JA 201). *Amnesty* involved a challenge to a different form of surveillance by plaintiffs who, the Supreme Court held, could not establish that the surveillance they complained of was taking place, or that it ever would, let alone that their own communications would be subject to it. This case, by contrast, involves a challenge to a fundamentally different—and far broader—form of surveillance, by plaintiffs who, because of unprecedented government disclosures, as well as the volume and dispersion of their own communications, can establish that the surveillance they complain of is taking place and that their own communications are already subject to it. The district court acknowledged some of the differences between Plaintiffs' suit and *Amnesty*, but it failed to recognize their significance. *See* Op. at 11–30 (JA 184–203).

Amnesty, which was filed the day that the FAA was enacted, involved a challenge to the statute on its face. The Supreme Court held 5-to-4 that the plaintiffs lacked standing to sue because they could not prove with sufficient certainty that they communicated with the NSA's surveillance targets. In *Amnesty*, the Supreme Court rejected the plaintiffs' standing theory as a "highly attenuated chain of possibilities," citing their inability to show: (i) that the government had sought FISC authority to engage in the surveillance at issue, (ii) that the FISC had granted the authority, or (iii) that their communications would be implicated by the surveillance. 133 S. Ct. at 1148–50.

This case differs from *Amnesty* in several crucial respects. First, the surveillance challenged here is fundamentally different from the surveillance challenged in *Amnesty*. As the Supreme Court described it, the plaintiffs in *Amnesty* challenged a form of targeted surveillance: they alleged that the NSA was "targeting" the communications of their contacts. In essence, they argued that the statute could be used to intercept their communications and that there was a significant likelihood it would be. The Supreme Court's standing analysis was predicated on the assumption that FAA surveillance implicated only those who were in direct contact with the NSA's targets. *See Amnesty*, 133 S. Ct. at 1148. Here, by contrast, Plaintiffs have challenged not targeted surveillance but a form of surveillance that involves the bulk copying and review of *essentially everyone's* international communications as those communications transit the internet backbone. There is no question here, given the detailed allegations in the Amended Complaint, that Plaintiffs' communications are being copied and reviewed. *See supra* Sections I.B–C. This fact alone brings this case outside the ambit of *Amnesty*.

Second, whereas the plaintiffs in *Amnesty* based their allegations almost entirely on what could be gleaned from the face of the statute, Plaintiffs' challenge here is informed by the government's unprecedented disclosures about its surveillance activities since *Amnesty* was decided. At the time *Amnesty* was litigated, virtually nothing had been revealed to the public about the way the FAA had been implemented. Again, the assumption of the Supreme Court was that the statute was being used to intercept only the communications of "targets." *See Amnesty*, 133 S. Ct. at 1148. Moreover, nothing was known about the NSA's practice of "about" surveillance because the government had not publicly discussed the practice, the government did not disclose it to the Supreme Court, it had not been the subject of media reports, and it is not contemplated by the plain language of the statute. Compl. ¶¶ 50–51 (JA 44–45).[18] Indeed, in *Amnesty*, the plaintiffs could not show that the FISC had authorized *any* FAA surveillance—or even that the government had sought such authorization. *See* 133 S. Ct. at 1148–50.

Here, by contrast, Plaintiffs' allegations about the government's surveillance are based almost entirely on the government's own disclosures since *Amnesty*.

[18] *See* PCLOB Report 84 ("The fact that the government engages in such collection is not readily apparent from the face of the statute, nor was collection of information 'about' a target addressed in the public debate preceding the enactment of FISA or the subsequent enactment of the FISA Amendments Act" in 2008).

Since 2013, the government has released multiple FISC opinions describing Upstream surveillance in detail, and the PCLOB examined Upstream surveillance at length in a comprehensive public report.[19] The government's disclosures also include public testimony by intelligence officials; multiple transparency reports; minimization procedures used by the NSA; and an executive-branch compliance assessment.[20] These disclosures establish that the government has implemented the FAA broadly, that it is engaged in Upstream surveillance, that Upstream surveillance involves "about" surveillance, and that "about" surveillance entails the copying and review of at least some of Plaintiffs' communications—and indeed that it involves the copying and review of substantially all communications in and out of the United States. *See supra* Sections I.B–C.

Third, while some of Plaintiffs here were plaintiffs in *Amnesty*, Wikimedia was not a plaintiff in the earlier suit, and the volume and distribution of Wikimedia's communications place this case on an entirely different footing. As discussed above, the fact that Wikimedia communicates with hundreds of millions of users spread across the globe makes it a virtual certainty that some of its communications are being monitored. While the technological issues in this case are more complex than were the issues before the Court in *Amnesty*, the standing inquiry here is far simpler. Given the massive quantity and comprehensive distribution of Wikimedia's communications—and given what has been revealed about the scope of Upstream surveillance—it is not just plausible but a virtual certainty that at least some of Wikimedia's communications are implicated by this surveillance.[21]

---

[19] *See, e.g.*, [*Redacted*], 2011 WL 10945618; *In re DNI/AG Certification* [*Redacted*], No. 702(i)-08-01 (FISC Sept. 4, 2008), http://1.usa.gov/20UeBig; PCLOB Report.

[20] *See generally* PCLOB Report (citing numerous official sources concerning Upstream surveillance).

Each of the differences identified above might be sufficient in itself to bring this case outside the holding in *Amnesty*, but the combination of them certainly does. Plaintiffs' standing argument does not rely on a "speculative chain of possibilities," Op. at 16 (JA 189) (quoting *Amnesty*, 133 S. Ct. at 1150). Here, unlike in *Amnesty*, the government has acknowledged engaging in the form of surveillance that Plaintiffs challenge. There is no question that the FISC has authorized the surveillance. *See* [*Redacted*], 2011 WL 10945618. And, critically, because of the nature of Upstream surveillance and the volume and distribution of Plaintiffs' communications, it is clear that Plaintiffs' communications are subject to Upstream's bulk copying and review. Indeed, to hold that *Amnesty* bars this case, as the district court did, is to mistake *Amnesty*'s fact-bound analysis for a kind of immunity rule that would place intrusive and far-reaching forms of surveillance beyond meaningful judicial review. *Amnesty* did not adopt any such rule. *See* 133 S. Ct. at 1150 n.5; *accord Susan B. Anthony List*, 134 S. Ct. at 2341.

---

[21] The Supreme Court recognized in *Amnesty* that a factual showing different from the one then before it could produce a different result. 133 S. Ct. at 1154. As discussed below, the NACDL defense attorneys whose clients have received notices of FAA surveillance are also in a far different position than the plaintiffs in *Amnesty*. *See infra* Section III.A; Compl. ¶¶ 112–29 (JA 65–72).

The district court's ruling is particularly perplexing given that *Amnesty* was decided on summary judgment whereas this case was decided on a motion to dismiss. As noted above, the governing legal standard at this stage of the case is well-established: the reviewing court must accept all non-conclusory allegations as true and draw "*all* reasonable inferences" in the plaintiff's favor. *Cooksey*, 721 F.3d at 234 (emphasis added); *Lucas v. S. Carolina Coastal Council*, 505 U.S. 1003, 1012 n.3 (1992) (holding that even "a generalized allegation of injury in fact" suffices "at the pleading stage"). This standard reflects a recognition that, at the pleading stage, a plaintiff will not yet have had the opportunity to present a complete record or engage in discovery. *See SD3*, 801 F.3d at 434. Thus, although the requirements of standing do not change from pleadings to trial, the manner of proof unquestionably does. *See Susan B. Anthony List*, 134 S. Ct. at 2342; *Jerome B. Grubart, Inc. v. Great Lakes Dredge & Dock Co.*, 513 U.S. 527, 537–38 & n.3 (1995). Here, the district court refused to draw *any* inferences in Plaintiffs' favor—let alone all reasonable ones. Rather than apply the motion-to-dismiss standard, the district court simply mischaracterized even reasonable inferences and factually detailed allegations as "fatal" speculation. *See, e.g.*, Op. at 18–19 (JA 191–92). This was in error.

III. Plaintiffs have plausibly alleged standing for additional reasons.

A. Plaintiffs have plausibly alleged that they have been compelled to take burdensome and costly measures in response to Upstream surveillance.

Plaintiffs have plausibly alleged that they have been forced to take burdensome and costly measures as a result of Upstream surveillance—a separate injury in fact sufficient to confer standing. *See Monsanto v. Geertson Seed Farms*, 561 U.S. 139, 154–55 (2010); *Friends of the Earth v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 184–85 (2000); Compl. ¶ 75 (JA 52). *Amnesty*, again, is not to the contrary. There, the Supreme Court explicitly recognized that a plaintiff may establish standing by showing that he or she has had to incur costs to mitigate a substantial risk of harm. *See* 133 S. Ct. at 1150 n.5. The Court concluded, however, that because the risk of surveillance in that case was based on an attenuated chain of contingencies, the plaintiffs' preventative measures did not confer standing. *See id.* at 1151. But the surveillance the government has acknowledged in this case is of a wholly different character—involving the bulk copying and review of international text-based internet communications. It is surveillance that has been authorized by the FISC, described in unprecedented detail, and is presently ongoing. As explained in the Amended Complaint, Plaintiffs are taking burdensome and sometimes costly measures in response to the virtual certainty that their communications are being copied and reviewed in the course of Upstream surveillance. *See, e.g.*, Compl. ¶¶ 67, 71, 109, 118, 128, 134, 144, 154, 164 (JA 50, 52, 64, 67, 71, 73, 76, 80, 83).

The necessity and reasonableness of these measures is clear given the implications of Upstream surveillance for Plaintiffs' constitutionally protected activities. For example, NACDL member and criminal defense attorney Joshua Dratel has a client, Agron Hasbajrami, whose communications the government has officially acknowledged intercepting and retaining using FAA surveillance. Compl. ¶ 121 (JA 68–69); Def. Mot. Dismiss 46 & n.31. Mr. Dratel had a second client, Sabirhan Hasanoff, whose prosecution also relied upon officially acknowledged FAA surveillance—in that case, involving the communications of another defendant in the same investigation. Compl. ¶ 121 (JA 68–69); Def. Mot. Dismiss 47. What this means is that the government's evidence in these criminal investigations was derived from FAA surveillance targeting one or more of the defendants' foreign contacts. *Amnesty* itself recognized that an attorney whose client received notice of FAA surveillance would "certainly have a stronger evidentiary basis" for standing than the plaintiffs in that case, because it would "be clear that the Government had acquired the foreign client's communications." 133 S. Ct. at 1154.

As a result of this acknowledged surveillance, Mr. Dratel's own international communications are especially likely to have been not only intercepted but retained—precisely because he is almost certain to have communicated with or about the same foreign individuals in the course of investigating the government's allegations, contacting witnesses, and collecting research and evidence from sources abroad via the internet. Compl. ¶ 127 (JA 70–71). In these circumstances, the rules of professional responsibility require Mr. Dratel to take reasonable precautions to maintain the confidentiality of his communications. *Id.* ¶ 128 (JA 71). Due in part to Upstream surveillance, in these representations and others, Mr. Dratel must employ burdensome electronic security measures to protect his communications, and in some instances he has to travel abroad to gather information in person. *Id.* These precautions are not "simply the product of [his] fear of surveillance," nor are they voluntary responses to a speculative threat. *Amnesty*, 133 S. Ct. at 1152. They are the product of surveillance the government acknowledged only after *Amnesty* was decided, including in cases where Mr. Dratel's client, his client's co-defendant, and key fact-witnesses overseas have been subject to FAA surveillance.[22]

[22] Contrary to the government's argument below, NACDL has identified a member who has suffered injuries in fact and, accordingly, NACDL has standing to sue on behalf of its members. *See S. Walk at Broadlands Homeowner Ass'n v. Openband at Broadlands, LLC*, 713 F.3d 175, 184 (4th Cir. 2013).

B. Plaintiffs have plausibly alleged that Upstream surveillance impairs their protected expressive activities.

As the Fourth Circuit has recognized, "First Amendment cases raise unique standing considerations that tilt dramatically toward a finding of standing." *Cooksey*, 721 F.3d at 235 (quoting *Lopez v. Candaele*, 630 F.3d 775, 781 (9th Cir. 2010)). "[W]hen there is a danger of chilling free speech, the concern that constitutional adjudication be avoided whenever possible may be outweighed by society's interest in having the [state action] challenged." *Sec'y of State v. Joseph H. Munson Co., Inc.*, 467 U.S. 947, 956 (1984). That Upstream surveillance impairs Plaintiffs' First Amendment activities supplies an independent basis for standing.

The Amended Complaint explains in detail how Upstream surveillance of Plaintiffs' communications infringes upon their First Amendment rights. Plaintiffs engage in a variety of First Amendment-protected activities, including journalism, advocacy, and the publication of educational material, and Upstream surveillance interferes with these activities in multiple ways. *See* Compl. ¶¶ 6–14 (JA 31–33). For Mr. Dratel, Upstream surveillance makes it expensive—and sometimes impossible—to obtain information necessary to his legal representations and advocacy. *See id.* ¶ 129 (JA 71–72). More broadly, the NSA's surveillance activities compel Plaintiffs to censor their own communications, and in some instances forgo electronic communications altogether. *See, e.g.*, *id.* ¶¶ 109, 128–29, 134, 139, 144, 149, 154, 159, 164 (JA 64, 71–73, 75–80, 82–84). These concrete harms are sufficient to support standing. *See Cooksey*, 721 F.3d at 235.

C. Plaintiffs have plausibly alleged that the NSA is not only copying and reviewing their communications, but retaining them as well.

Plaintiffs have plausibly alleged that there is a substantial likelihood that the NSA not only copies and reviews their communications, but retains them as well. That is because Plaintiffs communicate *about* persons and organizations targeted for Upstream surveillance, and because they communication *with* such targets. *See* Compl. ¶¶ 104–06, 115, 126, 133, 138, 143, 148, 153, 158, 163 (JA 61–63, 66, 70, 72–74, 76–81, 83).

As both the PCLOB and the FISC have observed, the breadth of the NSA's "about" surveillance means that the communications of innocent third parties are retained by the NSA if those communications happen to contain a targeted selector. *See* PCLOB Report 120. Thus, for instance, even viewing webpages that happen to contain a targeted selector can result in the NSA's retention of those internet communications. Because one of the Wikimedia Projects—Wikipedia—is an exhaustive encyclopedic resource, it includes entries related to virtually every foreign organization the U.S. government might target for Upstream surveillance. *See* Compl. ¶ 106 (JA 62–63). Website addresses or domain names associated with organizations on the U.S. State Department's Foreign Terrorist Organization list appear *over 700 times* on Wikimedia webpages—including within the encyclopedia entries describing organizations, like Uzbekistan's Islamic Jihad Union, whose communications the U.S. government has targeted using FAA surveillance. *Id.* Any time a user abroad visits or edits a page containing one of the government's targeted selectors, Wikimedia's communication with that user is very likely retained by the NSA. *Id.* ¶ 105 (JA 62). As this example shows, it is more than plausible that Plaintiffs communicate about NSA targets—and that Plaintiffs' communications are accordingly retained by the NSA.

Plaintiffs have also plausibly alleged a substantial likelihood that they communicate *with* some of the 92,707 individuals and organizations that are NSA targets. *See id.* ¶¶ 37, 71–73 (JA 39–40, 52). Given the identities and locations of Plaintiffs' contacts, there is a substantial likelihood that the NSA has targeted at least some of those contacts—and therefore has copied, reviewed, and retained Plaintiffs' communications. *See, e.g.*, *id.* ¶¶ 104–05, 115–16, 125, 127, 133, 138, 143, 148, 153, 158, 163 (JA 61–62, 66–67, 69–74, 76–81, 83). Because these are precisely the types of organizations and individuals that the government likely targets for foreign intelligence purposes, Plaintiffs have plausibly alleged a substantial likelihood that the NSA has targeted and retained their communications in the course of Upstream surveillance.[23]

---

[23] To be clear, Plaintiffs need not separately establish that their communications are being retained in order to challenge Upstream surveillance and the procedures that govern it. *See Berger v. New York*, 388 U.S. 41, 58–59 (1967); *Nat'l Treasury*

D. Wikimedia has plausibly alleged third-party standing to assert the rights of its community members.

Finally, although the district court did not address the question, Wikimedia has third-party standing to assert the rights of (1) U.S. persons abroad whose communications with Wikimedia are intercepted; and (2) individual users inside the United States, whose ability to exchange information with Wikimedia's foreign readers and editors has been impaired by Upstream surveillance. *Id.* ¶¶ 83–85, 98, 101, 108, 110 (JA 54–55, 59–61, 64–65); *see Kowalski v. Turner*, 543 U.S. 125, 129 (2004).

CONCLUSION

For the foregoing reasons, the district court's order dismissing Plaintiffs' Amended Complaint should be reversed.

February 17, 2016

Respectfully submitted,

/s/ *Patrick Toomey*

Patrick Toomey
Jameel Jaffer
Alexander Abdo
Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

Emps. Union v. Von Raab, 489 U.S. 656, 663, 675–76 (1989). While the retention of their communications is a further, discrete injury, Compl. ¶ 72 (JA 52), Plaintiffs have already shown that their communications are being copied and reviewed, and this is sufficient to give them standing to challenge the lawfulness of Upstream surveillance.

jeon@aclu-md.org

Charles S. Sims
David A. Munkittrick
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900
csims@proskauer.com

New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Counsel for Plaintiffs–Appellants

REQUEST FOR ORAL ARGUMENT

Due to the novel and significant legal issues in this case, Plaintiffs respectfully request oral argument pursuant to Local Rule 34(a).

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 13,839 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman.

/s/ Patrick Toomey
Patrick Toomey
Counsel for Plaintiffs–Appellants

Date: February 17, 2016

CERTIFICATE OF SERVICE

On February 17, 2016, I served upon the following counsel for Defendants–Appellees one copy of Plaintiffs–Appellants' BRIEF FOR PLAINTIFFS–APPELLANTS via this Court's electronic-filing system:

H. Thomas Byron, III
Catherine H. Dorsey
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530
Phone: (202) 616-5367
H.Thomas.Byron@usdoj.gov

/s/ Patrick Toomey
Patrick Toomey
Counsel for Plaintiffs–Appellants

Date: February 17, 2016